Office of Legislative Research
Research Report
February 3, 2016
2016-R-0008

OLR BACKGROUNDER: COMMERCIAL CYBER-SECURITY INSURANCE

By: Alex Reger, Legislative Analyst II

CYBER INSURANCE

A 2013 Experian report found that only 31% of companies have cyber-security insurance, and many companies that do purchase cyber-security insurance do not purchase enough to cover expected losses, according to a 2014 report by Marsh and McLennan Companies.

ISSUE

Explain commercial cyber-security insurance.

SUMMARY

Commercial cyber-security insurance typically covers a business' losses from a cyber-attack or loss of digital records containing personally identifiable information. It includes coverage for legal fees and court judgments, business interruption, cyber-extortion, and data loss, among other risks.

A report from Allianz estimates the cyber-security insurance market could reach $20 billion in annual premiums by 2025, and the cyber-security insurance industry is predicted to triple in size to $7.5 billion by 2020, according to a 2015 PricewaterhouseCoopers report. Nonetheless, the federal Department of Homeland Security's National Protection and Programs Directorate suggests the private cyber-security insurance market faces significant obstacles to growth, including the lack of actuarial data and the unpredictability of the cyber-sector.

Some insurers worry the exposure from cyber-attacks may be greater than the insurance industry's ability to underwrite the risk (an event called a "cyber-hurricane"). This has caused some insurers to avoid the commercial cyber-security insurance market.

According to the Insurance Department, cyber-security insurance appears to be purchased primarily by large businesses.

Phone (860) 240-8400
http://www.cga.ct.gov/olr
olr@cga.ct.gov

Connecticut General Assembly
Office of Legislative Research
Stephanie A. D'Ambrose, Director

Room 5300
Legislative Office Building
Hartford, CT 06106-1591

Small businesses are less likely to purchase cyber insurance or have preventive measures in place. As a result, they may be increasingly targeted for cyber-attacks and are less likely than large businesses to survive such an attack. A study by the National Cyber Security Alliance found that 60% of small businesses close within six months following a cyber-attack.

TYPES OF CYBER-LOSS

Cyber-security insurance primarily protects against two causes of cyber-loss: cyber-attacks, including cyber-crime, and privacy breaches.

Cyber-Attacks and Cyber-Crime

Cyber-attacks and cyber-crime are malicious attempts to damage or steal a company's networks, computer systems, or digital property. According to the Insurance Information Institute, losses from cyber-attacks and cyber-crime are increasing. The Center for Strategic and International Studies estimates the cost to the global economy from cyber-attacks and cyber-crime at $375 to $575 billion annually.

Privacy Breaches

Cyber-security insurance policies may also protect against privacy breaches. A privacy breach is the loss of digital records containing intellectual property or customers' or employees' personally identifiable information, even when such loss is accidental and not malicious. For example, an employee may lose a company laptop with sensitive information, or may accidentally send an email containing sensitive information to the wrong individual.

COMMERCIAL CYBER-SECURITY INSURANCE LIABILITY AND COVERAGE

Estimates of losses from cyber-attacks vary. A 2014 Ponemon Institute study found that the total direct and indirect cost of a cyber-attack to a U.S. company was approximately $5.85 million, or about $201 per compromised record. (Indirect costs include costs such as lost business due to diminished customer trust.)

Research suggests insureds with significant loss potential (e.g., insurance, retail, or healthcare companies that hold a lot of personally identifiable information) may not be purchasing enough cyber-insurance coverage. For example, one study of large retailers (i.e., businesses with revenue between $5 and $20 billion) found that such companies buy an average aggregate insurance limit of about $23 million. Such companies are estimated to have cyber-exposures ranging from $2.2 to $340 million. According to the Insurance Department, insureds wanting large amounts of

coverage (hundreds of millions) are likely to purchase several smaller policies from multiple insurers. Research infers this is because insurers are reluctant to offer policies with larger limits.

According to the Insurance Information Institute report, cyber-security insurance may cover a range of risks, such as:

1. business interruption — loss of business income resulting from a cyber-attack;
2. criminal rewards — the cost of a reward for information about a cyber-attack;
3. crisis management — public relations and reputation assistance;
4. customer notification and credit monitoring — expenses of notifying customers and offering credit monitoring;
5. cyber extortion — settlements of cyber-extortion threats;
6. data breach — expense and liability resulting from a cyber-attack;
7. data loss and corruption — damage or destruction of information;
8. identity theft — expenses related to the loss of personally identifiable information and account records;
9. liability — defense and litigation costs resulting from a cyber-attack; and
10. management liability — risks specific to management.

OBSTACLES TO GROWTH IN THE PRIVATE CYBER-INSURANCE MARKET

Actuarial Data, Premium Costs, and Policy Limits

Currently, insurers are offering only a limited range of cyber-insurance products primarily because of a lack of actuarial data and the unpredictability of the cyber-sector, according to a 2014 Department of Homeland Security report.

The lack of actuarial data results in incomplete actuarial tables, which makes it difficult to accurately predict potential risks and losses. According to the National Association of Insurance Commissioners, because of this lack of actuarial data insurers must qualitatively assess a business' risk and create a customized policy for the business. This may make cyber-insurance policies more expensive, with limited coverage options and low policy limits.

Premium costs and coverage options are derived from the size and scope of the business, the number of customers, and the type of data collected and stored, among other factors. Insurers may require insureds to adopt certain security protocols, which present additional costs for these businesses. (For example, just as living near a fire hydrant may reduce homeowners insurance premiums, having a secure firewall and antivirus may reduce cyber-security insurance premiums.)

At least some insurers support the creation of a national, anonymous cyber incident data set to alleviate these concerns.

Cyber Hurricane

A cyber-hurricane refers to a major cyber disaster resulting in more liability than insurers are capable of handling. According to an undated White House brief, the interdependent and standardized nature of computer systems make them vulnerable to highly correlated losses. The fear of a cyber-hurricane thus increases insurance premiums, creates barriers to market entry, and increases the cost of reinsurance.

SELECTED RESOURCES

Allianz Global Corporate & Specialty: A Guide to Cyber Risk. September 2015.

Center for Strategic and International Studies: Net Losses: Estimating the Global Cost of Cybercrime. June 2014.

Insurance Information Institute: Cyber Risks: Threat and Opportunities. October 2014.

Marsh and McLennan Companies: A Cybersecurity Call To Action. November 2014.

Ponemon Institute: *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age.* August 2013.

Ponemon Institute: 2014 Cost of Data Breach. May 2014.

PwC: Insurance 2020 & beyond: Reaping The Dividends Of Cyber Resilience. 2015.

AR:bs